21st Annual National Defense Industrial Association
Systems and Mission Engineering Conference

DoD Approach for Engineering Cyber-Resilient Weapon Systems and Program Protection

Melinda Reed

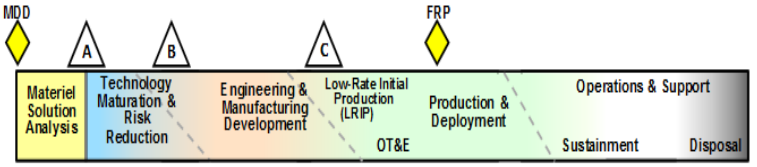
Office of the Under Secretary of Defense for
Research and Engineering

October 24, 2018

Ensuring Cyber Resilience In Defense Systems and Technologies

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - Found in programs, organizations, personnel, networks, systems, and supporting systems
  - Inherent weaknesses in hardware and software can be used for malicious purposes
  - Weaknesses in processes can be used to intentionally insert malicious hardware and software
  - Unclassified design information within the supply chain can be aggregated
  - U.S. capability that provides a technological advantage can be lost or sold
- ***Consequences:***
  - Loss of technological advantage
  - System impact – corruption and disruption
  - Mission impact – capability is countered or unable to fight through

Access points are throughout the Research and Engineering lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Contracting/Agree
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Key Protection Activities for Contested Cyberspace Environments

Program Protection & Cybersecurity

DoDI 5000.02, Enclosures 3 & 14

DoDM 5200.01, Vol. 1-4 | **DoDM 5200.45** | **DoDI 8500.01**

DoDI 5200.39 | **DoDI 5200.44** | **DoDI 5230.24** | **DoDI 8510.01**

Technology

What: A capability element that contributes to the warfighters' technical advantage (Critical Program Information (CPI))

Key Protection Activity:
- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

Goal: Prevent the compromise and loss of CPI

Components

What: Mission-critical functions and components

Key Protection Activity:
- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

Goal: Protect key mission components from malicious activity

Information

What: Information about the program, system, designs, processes, capabilities and end-items

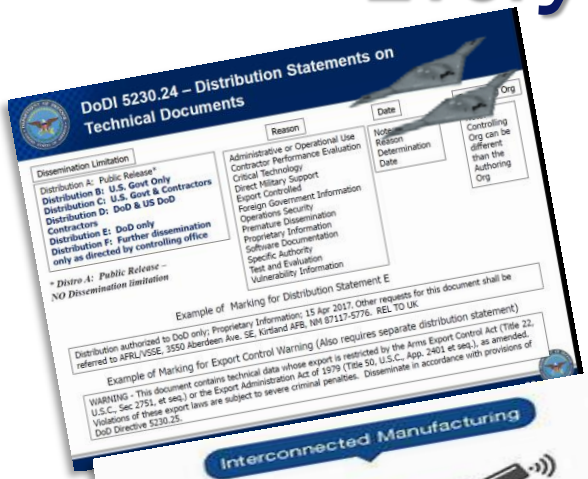
Key Protection Activity:
- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

Goal: Ensure key system and program data is protected from adversary collection

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: https://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Cybersecurity and Security Is Everyone's Responsibility



Everyone must take responsibility for cybersecurity from the *earliest research and technology development through system concept, design,* development, test and evaluation, production, fielding, sustainment, and disposal

Scope of cybersecurity includes:

- Program information Data about acquisition, personnel, planning, requirements, design, test data, and support data for the system
- Organizations and Personnel Government program offices, prime and subcontractors, along with manufacturing, testing, depot, and training organizations
- Networks Government, government support activities, and contractor owned and operated unclassified and classified networks
- Systems and Supporting Systems The system being acquired, system interfaces, and associated training, testing, manufacturing, logistics, maintenance, and other support systems

ENGINEERS
MAKE A WORLD OF DIFFERENCE

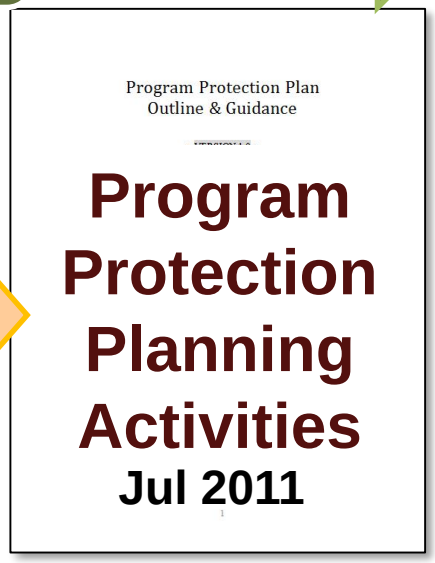
Cybersecurity and Security Protection Activity Relationships

COCOMS
- IPLS
- S&T IPLs

JCIDS
- Operational Needs
- Performance Criteria
- Operational Threats

Threats
- CI
- Intel

- TTRA
- ITA
- DIA TAC
- STAR
- Others



- Security Classification Guide
- Counterintelligence Support Plan
- Criticality Analysis
- Anti-Tamper Plan (If Applicable)
- Cybersecurity Strategy

Contracting Activities
- Trusted supplier requirements
- Acquisition regulations (Security, Safeguarding Covered Defense Information, Counterfeits, etc.)
- Foreign/International Engagement

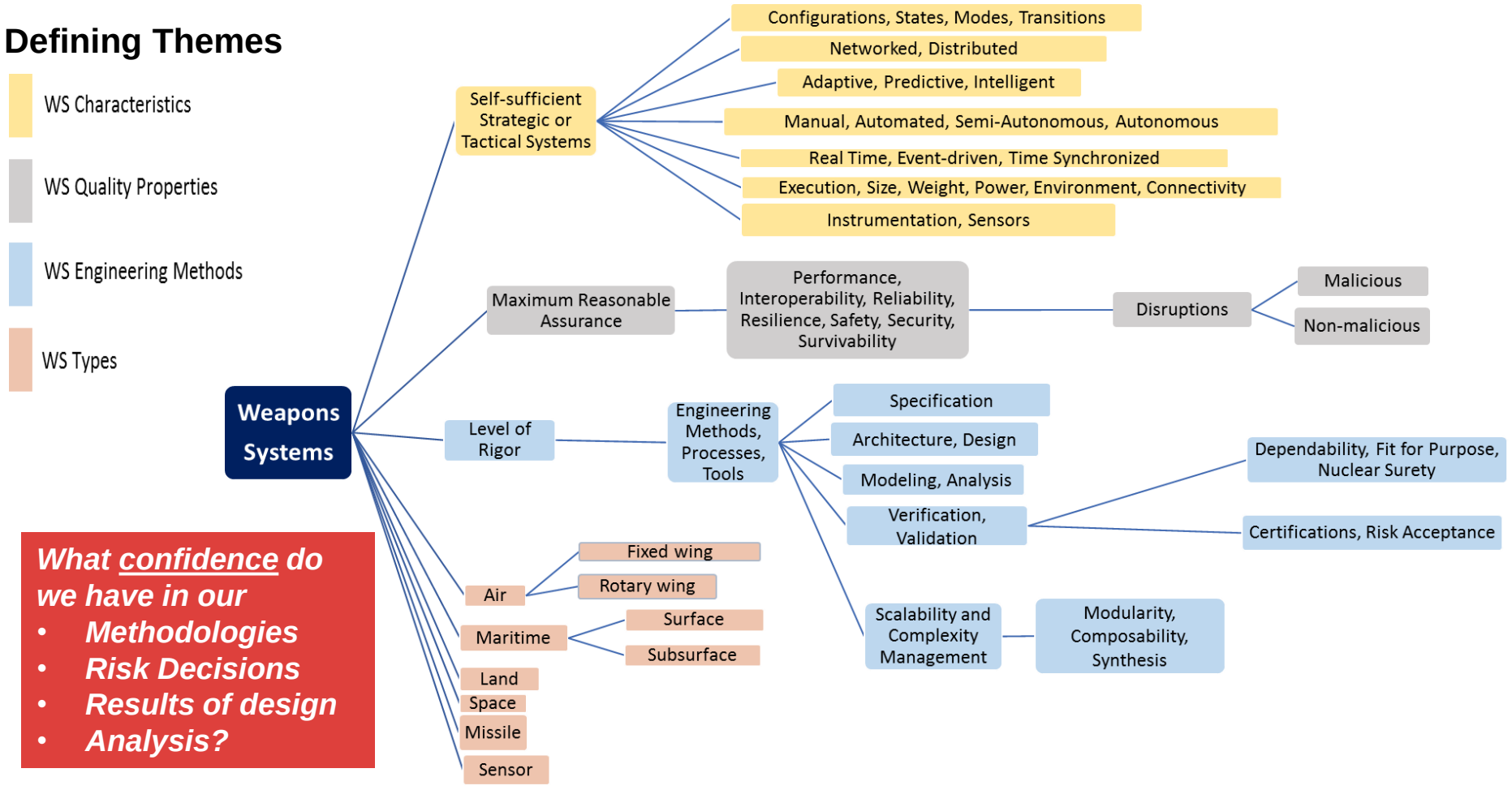
Engineering Activities
- Incorporation into technical baselines
- SSE entry and exit criteria in SE tech reviews
- SSE as a design consideration
- Technical risks and mitigation plans

Test Activities
- Data needed to ascertain cybersecurity requirements are met
- Cooperative Vulnerability Assessments
- Adversarial Assessments

Sustain & Maintain Activities
- Informs full life cycle protection activities for the program
- Lists critical components that require attention

Program Protection and Cybersecurity Considerations Are Integrated in All Aspects of the lifecycle

Weapon System Ecosystem
Concept to Deliver, Sustain, and Maintain



Weapon Systems Deliver Lethal Force with the Intent to Cause Harm

Implementing Cybersecurity into Weapon System Programs: Summary of Observations

- **PEOs, PMs and industry continue to report implementation is problematic.**
  - Acquisition programs are seeking clear and specific cyber resiliency guidance.
  - Risk Management Framework (RMF) for Information Technology (IT) governance and compliance schemes don't possess weapons and tactical domain expertise
- **Services and agencies, PEOs/programs, and industry partners are each working to determine cyber resiliency solutions.**
  - No common implementation of rules or principles; Solutions beginning to diverge
- **Operational Test community, Red Teams, COCOM exercises continue to identify vulnerabilities.**
  - Findings in legacy systems indicate that cybersecurity must be designed in, not tested in, nor patched in.
  - Developmental T&E is shifting left. Engineering needs to lay the foundation for the shift.

Core Recurring Challenges		
Design Guidelines	**Engineering Assessment**	**Implementation**

Addressing Core Challenges Through Engineering Cyber Resilient Workshops

Workshop 1 Findings

1. *Requirements derivation is a challenge area*
2. *Require clarity on Risk Acceptance*
3. *Assessments should be integrated with and driven by SE Technical Reviews*

Workshop 2 Findings

1. *Definitions, Taxonomy & Standards Framework*
2. *Knowledge Repository*
3. *Consolidated Risk Guide*
4. *Assessment Methods*
5. *Needs Forecasting*
6. *Industry Outreach*

Workshop 3 Actions

1. *Establish DAU CRWS CoP; facilitate definitions, taxonomy standards*
2. *Develop Risk, Issues, & Opportunities engineering cyber appendix*
3. *Align assessment approaches*
4. *Explore S&T opportunities*
5. *Address Workforce needs*
6. *Industry Outreach*

Workshop 4 Actions

1. *Cyber effects on Technical Performance Measures and Metrics*
2. *Examine cyber requirements and SETR criteria*
3. *Leverage System Safety*
4. *Identify considerations for embedded software*
5. *Inform RIO based on cyber effects*

Workshop 5 Actions

1. *Integrate supply chain mitigation approaches in standards, guidance and assessment methods*
2. *Considerations in modernization of systems in sustainment*
3. *Plan for sustainment*
4. *Use available validated Intelligence and counterintelligence to make risk informed decisions*

Workshop 6 Actions

1. *Develop Foundations, Principles & Concepts, and Practices*
   - *Integrate across specialty and security domains*
   - *Broad applicability for core commonality in application*
   - *Practices reflect application in "type-specific" context*

Engineering Cyber Resilient Weapon System Workshop Key Findings and Actions

Design for Cyber Threat Environments Early Development Through Sustainment

Allocate cybersecurity and related system security requirements to the system architecture; design and assess for vulnerabilities.

The system architecture and design will address, at a minimum, how the system:

- Manages access to and use of the system and system resources
- Is structured to protect and preserve system functions or resources, (e.g., through segmentation, separation, isolation, or partitioning)
- Is configured to minimize exposure of vulnerabilities that could impact the mission, including through techniques such as design choice, component choice, security technical implementation guides and patch management in the development environment (including integration and T&E), in production and throughout sustainment.
- Monitors, detects, and responds to security anomalies.
- Maintains priority system functions under adverse conditions; and
- Interfaces with DoD Information Network (DoDIN) or other external security services

Key Design Activities to Mitigate Cybersecurity Risks to the System

Utilize Engineering Building Blocks

Approaches to Address Core Cybersecurity Challenges in Weapon Systems

- **Cybersecurity requirements derivation and analysis**
  - Treat cybersecurity as an aspect of system performance
  - Integrate cybersecurity concerns into requirements analysis
  - Correlate security requirements analysis with all levels of design and associated systems analysis
- **Technical Performance Measures (TPMs)**
  - Determine the effect cyberspace has on achievement of existing TPMs
  - Determine the extent of effectiveness of existing methods
  - Determine the need for methods to address the gap
- **Weapon System Software**
  - Apply sound software engineering, computer science, and software development principles and methods to reduce unnecessary exposure and vulnerability
  - Differentiate software as a component and software as a system
  - Evolve methods informed by system safety to address the software contribution to security risk
- **DoD Risk, Issue, and Opportunity (RIO) Management**
  - Integration of methods to address the adverse effects presented by cyberspace into Technical RIO methods
  - Differentiate cybersecurity risk and issue
  - Differentiate known and unknown scenarios that produce adverse effects

Build Upon Engineering Building Blocks

Approaches to Address Core Cybersecurity Challenges in Weapon Systems

- **Synergy with System Safety**
  - Adopt approaches and methods of system safety to improve cybersecurity engineering
  - Achieve increased synergy across the approaches and methods of safety and security engineering
- **System Engineering Technical Review (SETR) Criteria**
  - Establish criteria sufficient to make informed decisions about the safe, secure, and resilient aspect of achieving capability and performance objectives
- **Workforce Development**
  - Establish roadmap and curriculum to educate and train today's and tomorrow's engineering workforce for more effective technical engineering planning and execution in response to challenges presented by cyberspace

- **Standardize Practices and Approaches**
  - Establish Standards Area under Defense Standardization Program to standardize direction to industry in contracting

Weapon System Assurance

- **Claims are stated relative to**
  - Design intent (the norm)
  - Cases of disruption and subversion (deviation from norm)
- **Insufficient confidence translates to risk**
  - DoD MIL-STD-882E
  - NASA System Safety

Assurance is: Justified confidence that a claim has been or will be achieved [IEEE 15026]

Loss-Driven Engineering Approach

- **Loss is the basis for security activities and judgments**
  - Security protection needs arise in direct response to a loss effect
    - Avoid and prevent
    - Minimize the extent and/or duration of
    - Recover from
- **Scope of loss includes:**
  - Death, injury, or occupational illness
  - Damage to or loss of equipment or property
  - Damage to or loss of data or information
  - Damage to or loss of capability, function, or process
  - Damage to the environment

Drive Engineering into Cybersecurity

Emerging Engineering Focus Areas

- **Security System Analysis**
  - Loss-driven analysis to determine the effects of cyberspace and the effectiveness of solutions
  - Balanced application of threat data-dependent and threat data-independent methods
  - Application of appropriate rigor to continuously build confidence
  - **Lexicon and Taxonomy**
    - Expand what we have and provide distinct clarity rather than expand and abstract “things cyber”
    - Refine and deconflict security terminology
    - Provide trace and translation where synonymous lexicon and taxonomy of other specialties
    - **Secure Design Foundations**
      - Codify idealized design foundations and principles for security
        - Leverage sources that span seminal work in computer security to current work on resilience
        - Derive principles that underlie security controls and trace to the design foundations
      - Apply the foundation and principles for security in context
    - **System Resilience**
      - Characterize resilience as an attribute of delivered capability
      - Develop concept of resilience scenarios and correlate to loss scenarios
      - Develop concepts for resilience requirements and their representation

Evolve Engineering Methodologies

- **Focus on design for assurance to realize safe, secure, and resilient weapon system capability.**
- **Prioritize the design on the delivered capability and achieving capability performance objectives with acceptable risk.**
  - What the system does/does not do and purpose of the system
  - All normal and contingency system states/modes
- **Design with considerations on how the system effects delivered capability.**
  - The inherent system exposure, hazard, and vulnerability
  - The nature of how the system fails and behaves when stressed or subjected to adversity
- **Differentiate causal factors and conditions that result in loss from risk and issue activities and decision-making to address loss.**
- **Continuously build confidence about the ability to prevent, control, constrain loss.**

Add Engineering Considerations into Cybersecurity

Summary

- **Each system is different, each operational environment is different; approaches must be tailored to meet the requirement, operational environment and the acquisition.**
  - We will embed cybersecurity risk mitigation activities into the acquisition program lifecycle.

- **We must continue to mature policy, tools, and expertise to design cyber resiliency in our systems.**
  - Translate IT and network resiliency to weapon system resiliency.

- **Opportunities for government, industry and academia to engage:**
  - Use loss-driven analysis to determine the effects of cyberspace and the effectiveness of solutions
  - Determine the effect cyberspace has on achievement of existing TPMs
  - Characterize resilience as an attribute of delivered capability
  - Adopt approaches and methods of system safety to improve cybersecurity engineering

DoD Research and Engineering Enterprise
Solving Problems Today – Designing Solutions for Tomorrow










DoD Research and Engineering Enterprise
https://www.acq.osd.mil/chieftechnologist/

Defense Innovation Marketplace
https://defenseinnovationmarketplace.dtic.mil

Twitter
@DoDInnovation

For Additional Information

Melinda Reed

Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))

571.372.6562 | melinda.k.reed4.civ@mail.mil

Program Protection and Cybersecurity in DoD Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Assigns and prescribes responsibilities for Cybersecurity, includes security, to the acquisition community
- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD; PM will submit PPP for *Milestone Decision Authority approval* at each Milestone review

DoDI 5200.39 Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation

- Establishes policy and responsibilities for identification and protection of critical program information
- Protections will, at a minimum, include anti-tamper, exportability features, security, cybersecurity, or equivalent countermeasures.

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

- Establishes the DoD Cybersecurity Program, the DoD Principal Authorizing Official and Senior Information Security Officer to achieve cybersecurity through a defense-in-depth approach that integrates personnel, operations, and technology